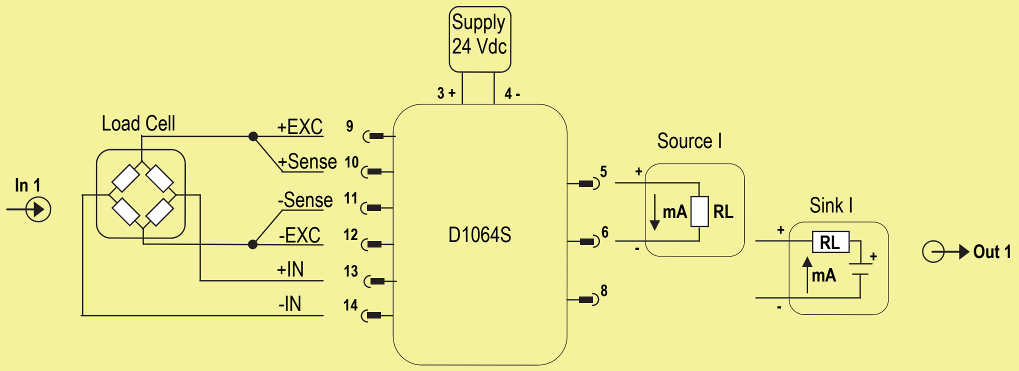
SAFETY MANUAL

SIL 2 Load Cell/Strain Gauge Bridge
Isolating Converter
Din-Rail Model D1064S

Reference must be made to the relevant sections within the instruction manual ISM0088,
which contain basic guides for the installation of the equipment.

technology for safety

Application for D1064S - with 4-20 mA current source (or sink) output .



Description:

The module is powered by connecting 24 Vdc power supply to Pins 3 (+ positive) - 4 (- negative). The green LED is lit in presence of supply power.
Connect load cell or strain gauge bridge voltage supply at terminal “9” positive and terminal “12” negative.
Connect load cell or strain gauge bridge voltage sensing supply at terminal “10” positive and terminal “11” negative.
If load cell or strain gauge bridge has no internal voltage sensing capability always connect terminal "10" to terminal "9" and terminal "11" to terminal "12"; for better performance connect the wire at the end of the line near the load cells.
Connect load cell or strain gauge bridge output signal at terminal “13” positive and terminal “14” negative.
Connect current source mode positive output at terminal “5” and negative output at “6” or current sink mode positive output at terminal “6” and negative output at terminal “8” (output can be used only one type at a time, not contemporary).

Safety Function and Failure behavior:

D1064S is considered to be operating in Low Demand mode, as a Type B module, having Hardware Fault Tolerance (HFT) = 0.
The failure behavior of D1064S module with 4-20 mA current source (or sink) output is described by the following definitions:

- Fail-Safe State: is defined as the output going to 0 mA due to module shutdown;
- Fail Safe: failure mode that causes the module / (sub)system to go to the defined fail-safe state without a demand from the process;
- Fail Dangerous: failure mode that does not respond to a demand from the process or deviates the output current by more than 5% (± 0.8 mA) of full span.
- Fail High: failure mode that causes the output signal to go above the maximum output current (> 20 mA). Assuming that the application program in the Safety logic solver is configured to detect High failure, this failure has been classified as a dangerous detected (DD) failure.
- Fail Low: failure mode that causes the output signal to go below the minimum output current (< 4 mA). Assuming that the application program in the Safety logic solver is configured to detect Low failure, this failure has been classified as a dangerous detected (DD) failure.
- Fail Dangerous Detected: it’s a dangerous failure which has been detected from module internal diagnostic so that output signal is forced below the minimum output current < 4 mA (as Fail Low) or above the maximum output current > 20mA (as Fail High).
- Fail “No Effect”: failure mode of a component that plays a part in implementing the safety function but that is neither a safe failure nor a dangerous failure. When calculating the SFF, this failure mode is not taken into account.
- Fail “Not part”: failure mode of a component which is not part of the safety function but part of the circuit diagram and is listed for completeness. When calculating the SFF this failure mode is not taken into account.

As the module has been evaluated in accordance with Route 2H (proven-in-use) of the IEC 61508:2010, Diagnostic Coverage DC ≥ 60% is required for Type B elements.
Being HFT = 0, in Low Demand mode the maximum achievable functional safety level is SIL 2.
Failure rate date: taken from Siemens Standard SN29500.

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	155.71
λ_{du} = Total Dangerous Undetected failures	81.53
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	77.98
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**315.22**
MTBF (Safety Function, single channel) = (1 / $\lambda_{tot\ safe}$) + MTTR	**362 years**
λ_{ne} = “No Effect” failures	196.48
λ_{np} = “Not Part” failures	31.40
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{ne} + \lambda_{np}$	**543.10**
MTBF (Device) = (1 / $\lambda_{tot\ device}$) + MTTR	**210 years**

Failure rates table according to IEC 61508:2010 Ed.2:

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	DC	SFF
0.00 FIT	77.98 FIT	155.71 FIT	81.53 FIT	65.63%	74.14%

where DC means the diagnostic coverage for the input sensor by module internal diagnostic circuits and by Safety logic solver. This type “B” system, operating in Low Demand mode with HFT = 0, has got DC = 65.63 % ≥ 60 % as required by Route 2H evaluation (proven-in-use) of the IEC 61508:2010.

PFDavg vs T[Proof] table (assuming Proof Test coverage of 99%), with determination of SIL supposing module contributes ≤ 10% of total SIF dangerous failures:

T[Proof] = 1 year	T[Proof] = 2 years
PFDavg = 3.59 E-04 - Valid for **SIL 2**	PFDavg = 7.18 E-04 - Valid for **SIL 2**

PFDavg vs T[Proof] table (assuming Proof Test coverage of 99%), with determination of SIL supposing module contributes > 10% of total SIF dangerous failures:

T[Proof] = 10 years
PFDavg = 3.59 E-03 - Valid for **SIL 2**

SC 2: Systematic capability SIL 2.

Testing procedure at T-proof

The proof test shall be performed to reveal dangerous faults which are undetected by diagnostic.
This means that it is necessary to specify how dangerous undetected faults, which have been noted during the FMEDA, can be revealed during the proof test.

Proof test 1 (to reveal approximately 50 % of possible Dangerous Undetected failures in the converter)

Steps	Action
1	Bypass the Safety-related PLC or take any other appropriate action to avoid a false trip.
2	Set the input load cell to the High (see Safety Function definition) voltage and verify that the related analog output current reaches the corresponding value. This test is for voltage compliance problems, such as a low power supply voltage or an increased wiring resistance, and for other possible failures.
3	Set the input load cell to the Low (see Safety Function definition) voltage and verify that the related analog output current reaches the corresponding value. This tests is for possible quiescent current related failures.
4	Restore the loop to full operation.
5	Remove the bypass from the safety-related PLC or otherwise restore normal operation.

Proof test 2 (to reveal approximately 99 % of possible Dangerous Undetected failures in the converter)

Steps	Action
1	Bypass the Safety-related PLC or take any other appropriate action to avoid a false trip.
2	Perform steps 2 and 3 of **Proof Test 1**.
3	Perform a two-point calibration (i.e. down and full scale) of the connected load cell and verify that, forcing some values of the input range, the module output current related values are within the specified accuracy (5 % (± 0.8 mA) of full span) as defined in the Safety Function. This requires that the input load cell has already been tested without the converter and does not contain any dangerous undetected failures.
4	Restore the loop to full operation.
5	Remove the bypass from the safety-related PLC or otherwise restore normal operation.